STREAM CIPHER DESIGN WITH REVOLVING BUFFERS

Techniques are disclosed to limit short-term correlations associated with outputs of stream cipher keystream generators. Output values of a generator are paired such that the paired outputs are sufficiently far apart to be considered independent. In one described implementation, a method includes sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units. A pairing function pairs individual values from the first and third storage units that are at least a threshold value apart. Upon reaching the threshold value of the output rule results, the contents of the first, second, and third storage units are rotated serially.